REMARKS

Reconsideration of the rejection of the claims in this application is respectfully requested. Currently, claims 1, 3-10, and 12-18 are pending in this application.

Rejection of claims under 35 USC 103 over Ma in view of Shah

Claims 1, 3-10, and 12-18 were rejected under USC 103 over Ma (U.S. Patent No. 5,953,338) in view of Shah (U.S. Patent No. 6,678,835). This rejection is respectfully traversed in view of the following arguments.

1. The policy server 122 of Shah is not a VPN server that authenticates, encapsulates, and/or de-encapsulates packets.

As set forth in applicant's recently filed Appeal Brief, this application relates to a method for a server to manage bandwidth of a link not directly connected to the server, to enable differentiate classes of service of traffic to use the link without requiring modification of routers forming a path through the network. (Specification at p. 2, lines 6-7). By allowing the server to meter bandwidth on a per-application group basis, different application groups can share a link fairly by causing packets within an application group to contend for bandwidth allocated to that application group, and to not contend for bandwidth allocated to other application groups. (Specification at p. 4, line 21 to p. 5, line 4). This is advantageous in that it allows a server on a network to control how different application groups contend for limited bandwidth on a link that is not connected to the server, such as when the server is configured to control how much bandwidth each application group will be allowed to use on an access link connecting a local area network to an external network (Specification at p. 4, lines 21-29).

Independent claim 1 recites a method that includes the steps of assigning by the VPN server a portion of bandwidth of a remote link to at least one application group, and then metering by the VPN server packets belonging to the application group. Additionally, claim 1 recites that the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets. Thus, to find the method of claim 1 obvious, the Examiner must show that it would have been obvious to create a VPN server that would perform both of these steps. Applicants respectfully submit that a person of ordinary skill in the art would not have found it obvious to do so when faced with the same problem, and with the knowledge of both Ma and Shah.

The Examiner has taken the position that Ma discloses a system for managing bandwidth of a remote link in a VPN 170 (Fig. 1) comprising a server 160 (Fig. 2, Col. 7 lines 5-14), a contention pool 401 or 402 having a portion of the bandwidth for at least one application group (Fig. 4A Col. 11 lines 11-26) and a meter 145 for metering the packets belonging to the application group. The Examiner admits that Ma fails to teach that the server is a VPN server configured to authenticate, encapsulate or de-encapsulate at least a portion of the packets, but contends that Shah teaches such a VPN server (citing Fig. 1, Col. 6, lines 13-32). Thus, the Examiner concludes that it would have been obvious to employ "the policy server 122 with VPN processing as taught by Shah" in Ma's server 160. As motivation to make the combination, the Examiner has cited Col. 6, lines 33-42 of Shah. Applicants respectfully submit that the combination of Ma and Shah would not have rendered the claims of this application obvious because the "policy server 122" in Shah is not a VPN server that is configured to authenticate, encapsulate or de-encapsulate packets.

The policy server 122 in Shah does not handle packets. Rather, the policy server 122 in Shah is used to define policies that are passed to the policy enforcers 124. The policy enforcers 124 are edge routers that actually handle the packets. Specifically, Shah teaches a system that includes a central policy server in communication with first and second edge devices. (Col. 1, lines 66-67). The central policy server manages the first and second edge devices from a central location to cause the edge devices to implement policy. This enables policy to be defined and managed from a single location (Col. 1, at lines 46-48). Examples of policies that may be defined are set forth at Col. 4, lines 13-32. The policies are defined by the policy server 122 (Col. 4, lines 13-15) and enforced by an edge device, which is referred to in Shah as a policy enforcer 124. (Col. 4, lines 33-42). The policy enforcer thus is the entity that is handling packets on the network in connection with controlling access to the network, whereas the policy server 122 is a central control system configured to instruct the policy enforcer how to handle particular types of traffic. Id.

As support for the Examiner's position that the central policy server 122 handles packets, the Examiner has cited Shah at col. 6, lines 13-32, and Figs. 1-2. For convenience, this portion of Shah is reproduced below:

> According to one embodiment of the invention, a policy object 222 includes a bandwidth policy 224, firewall policy 226, administration policy 228, and VPN policy 230. The VPN policy 230 defines a security policy for the member networks and includes one or more VPN clouds 232. Each VPN cloud 232 is an individual VPN or a group of VPNs defining a security policy group which includes a list of sites 234 and users 236 who can communicate with each other. A site is preferably a set of hosts/networks physically located behind one of the policy enforcers 124, 126. In other words, a site is a definition of a network which includes the policy enforcer that is associated with it. The policy enforcers for the sites act as VPN tunnel endpoints once the hosts under the sites start communicating. These communications are governed by a set of rules 238 configured for each VPN cloud. The rules 238 may govern, among other things, VPN access permissions and security features such as the level of encryption and authentication used for the connectivity at the network layer.

As is clear from this passage, the VPN cloud includes a set of hosts/networks that are physically behind a policy enforcer 124. The policy enforcer 124, as discussed above, is defined in Shah as an edge device that applies policies defined by a central policy server 122. (Col. 4, lines 33-42). Shah further states that the policy enforcer (edge device) acts as a VPN tunnel endpoint. Thus, the VPN policy server 122 of Shah is not configured to handle packets as asserted by the Examiner.

The policy server 122 in Shah is similar to the centralized control module in Ma in that it, like Ma's centralized control module, is used to set policy in a centralized manner. Thus, both references teach central servers that specify the policy to be implemented by routers, and neither reference teaches a VPN server that assigns a portion of the bandwidth of a remote link to an application group and then meters packets belonging to the application group. The VPN policy enforcer 124 of Shah does not perform this process, nor does the policy server 122 of Shah or the centralized control module of Ma. Accordingly, applicants respectfully submit that the claims are patentable over the combination of Shah and Ma.

2. <u>Ma and Shah do not teach management of a remote link.</u>

In Ma, the central control specifies policies that are to be enforced by routers, and those routers are directly connected to the links that are being controlled. Similarly, in Shah the central policy server specifies policy that is directly applied by policy enforcers 124. In neither instance is a network element controlling the flow of packets on the network to manage the bandwidth of a remote link. Accordingly, for this additional reason, applicants respectfully submit that the claims are patentable over the combination of Ma and Shah.

Conclusion

Applicant respectfully submits that the claims pending in this application are in condition for allowance and respectfully requests an action to that effect. If the Examiner believes a telephone interview would further prosecution of this application, the Examiner is respectfully requested to contact the undersigned at the number indicated below.

If any fees arc due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref: NN-13361).

Respectfully Submitted

John C. Gorecki
Registration No. 38,471

Dated: March 22, 2007

John C. Gorecki, Esq.
Patent Attorney
180 Hemlock Hill Road
Carlisle, MA 01741
Tel: (978) 371-3218
Fax: (978) 371-3219
john@gorecki.us